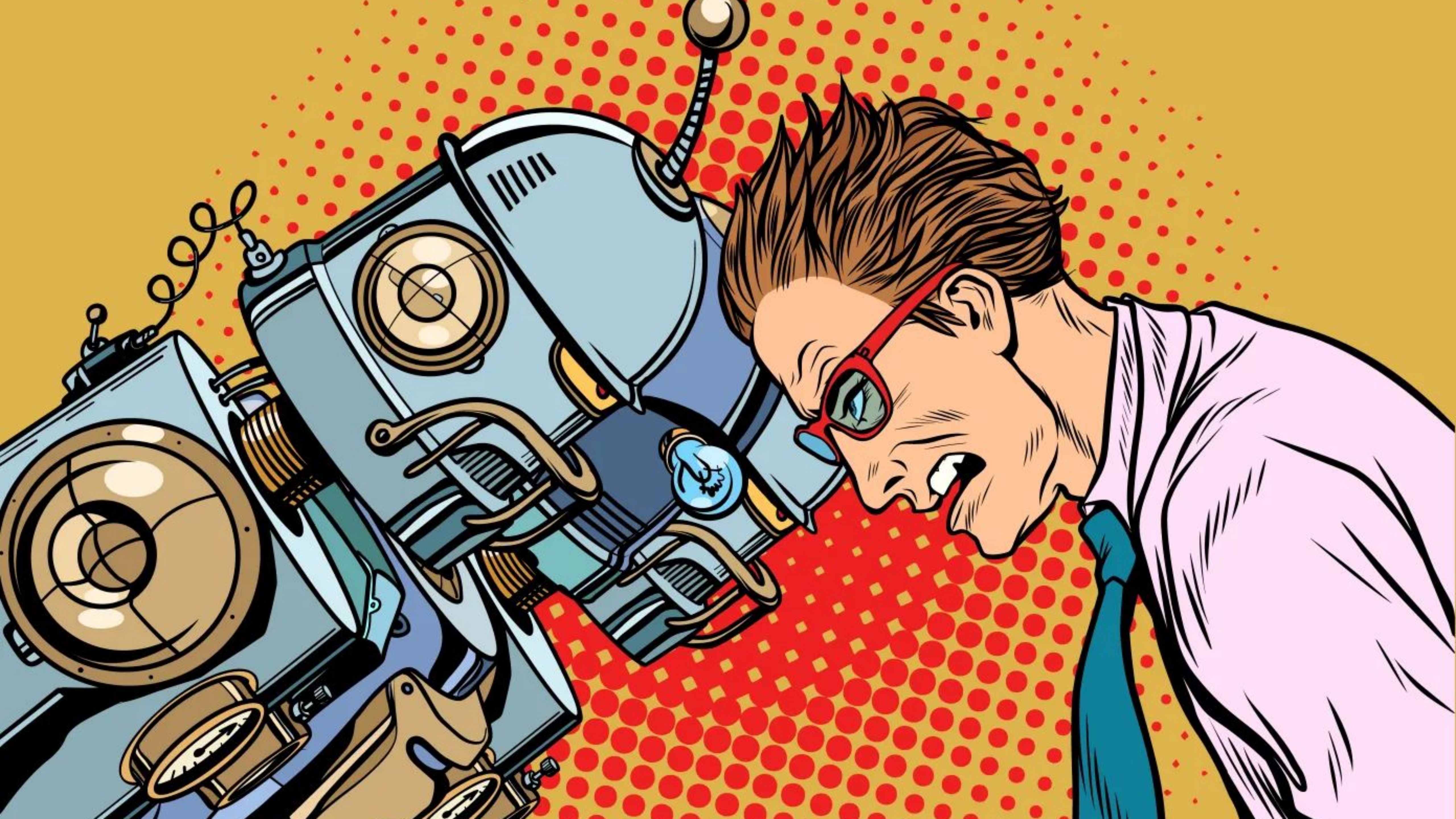


Защита от вредоносной автоматизации сегодня

Антон Лопаницын





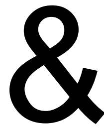
Боты

Полезные	Потенциально-опасные	Вредоносные
соцсети и мессенджеры, которые делают превью	индексирующие боты, которые не приносят трафик (shodan, censys)	сканеры уязвимостей и нетаргетированные эксплойты
системы аналитики и доступности сайтов	парсеры контента	DDoS-боты на L7-уровне
поисковые боты индексируют сайты	спам-боты	Кликботы, SMS-бомберы



Боты









Как определить, что боты среди нас?



Есть ли боты и сколько их

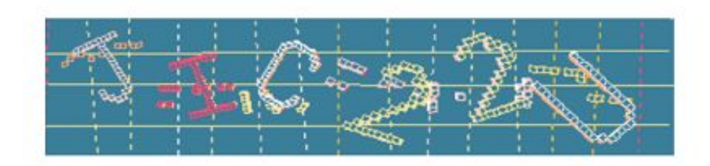
1. Смотреть в аналитику (или внедрять ее)
2. Забрать оттуда ключевые метрики пользователей
3. Разметить трафик
4. Внедрять защиту
5. Перейти к пункту 1, чтобы оценить усилия

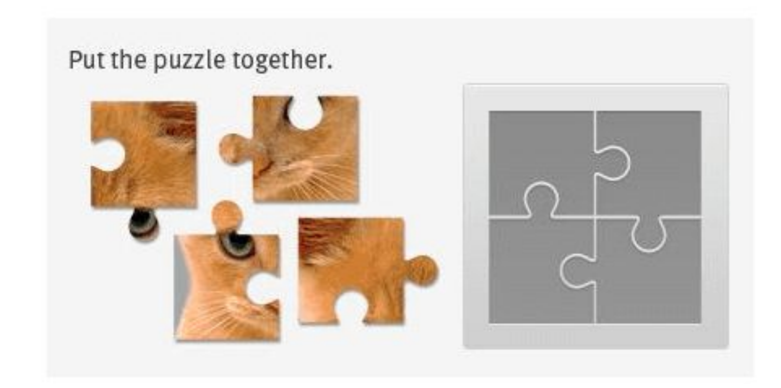


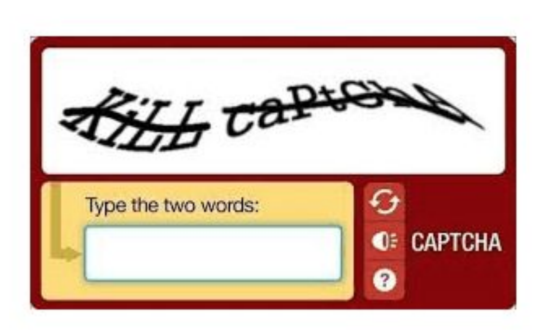
Методы противодействия автоматизации

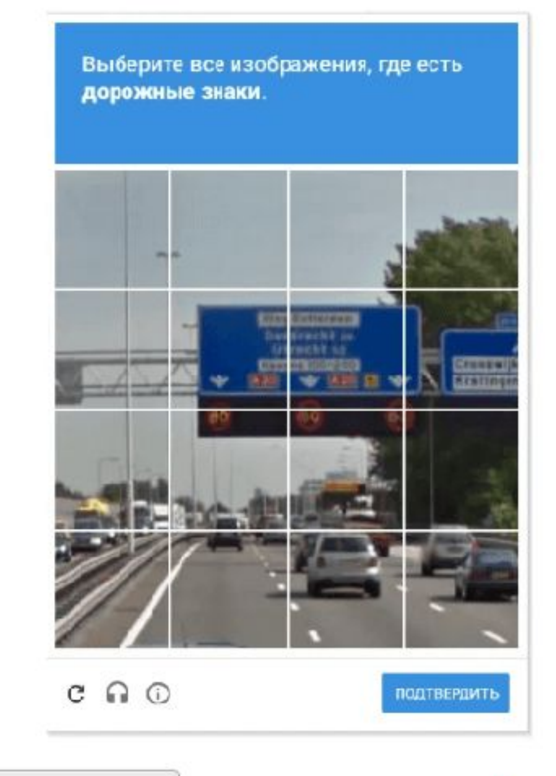


Captcha











Яндекс
Показать другую картинку

Пользователи — бесит. Бизнес — падает конверсия.

Парадокс, что капчу боты обходят быстрее людей.



Captcha

	Цена за 1 000	Успешность	Скорость решения
reCAPTCHA v2	$0,6	99%	10 s
reCAPTCHA v3	$0,9	99%	5 s
reCAPTCHA Enterprise	$1	97%	11 s
reCAPTCHA Enterprise Y! Yahoo Spotify	$4	98%	10.5 s
hCaptcha	$0,8	99%	11 s
FunCaptcha Beta	$0,6	91%	13 s
GeeTest Beta	$0,6	92%	23 s
TEXT Captcha	$0,3	99%	0.8 s

- Бьёт по UX
- Падает конверсия
- Низкая стоимость решения для злоумышленников

Мнение:
Применима в местах, где для успешной атаки нужны сотни тысяч действий*



Proof of Work



Checking your browser before accessing gitlab.com.

This process is automatic. Your browser will redirect to your requested content shortly.

Please allow up to 5 seconds...

Алгоритм для вычислений, который потребует много ресурсов от клиента, но легко проверяется на сервере.

Технология, состоящая из компромиссов.



Proof of Work

- Бьет по performance
- Стоимость типичной спамерской атаки почти не вырастает, если заставить его что-то считать
- Нужна поддержка маломощных (и старых устройств). А значит PoW злоумышленника будет считаться еще быстрее
- Можно посчитать PoW и использовать его на боте (и другие уязвимости)
- Надо вести белый список хороших ботов, чтобы не ломать превьюшки

Мнение: применим в случае DDoS-атаки на L7, если у вас есть такие атаки



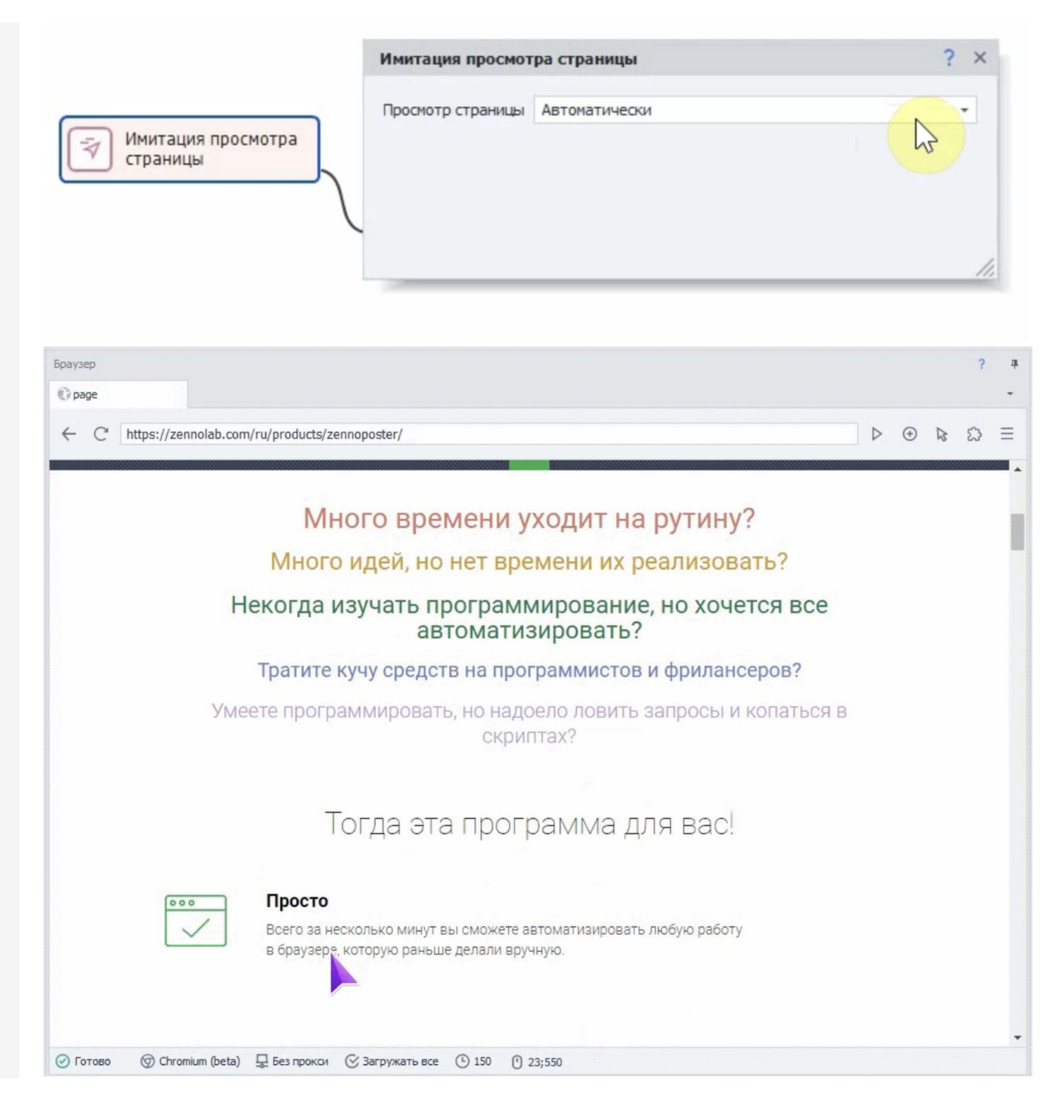
Анализ поведения

Анализ поведения не дает возможности построить модель, которая хорошо вычищает ботов, но не затрагивает пользователей.

Обучить нейронку и автоматизировать действия пользователей не дороже, чем построить аналитику.



Анализ поведения



- False positive, срезаем часть трафика
- False negative, оставляем часть ботов

Мнение: работает для аналитики, поиска аномалий, не работает для принятия решений.



Исторические факты



История пользователей, их действия, “порядочность”.
Скоринг-модель должна учитывать резкую смену поведения.

Если много денюшков — решения класса “сессионный антифрод”.



Исторические факты

- Для своего решения вы должны быть большими (рекламные пиксели, покупки, трекинг прочих действий)
- Решение на минималках — один из публичных вариантов recaptcha v3, smartcapcha
- Используются ботнеты или кража данных для накрутки “истории”
- Возможен реверс скоринговой модели (зайти в gmail, посмотреть ролик на youtube => увеличить скоринг в recaptcha)

Вывод: отлично работает, но и легко обходится.
Для новых пользователей или устройств ухудшается UX



Применимость подходов

Метод противодействия	Применимость	Проблемы	Преимущества
Captcha	Предотвращение множественных действий	Уменьшение конверсии, низкая стоимость обхода	Легкая интеграция
PoW	Отражение DDoS	Проблемы с старыми устройствами, околонулевая стоимость обхода	Возможно увеличивать сложность по мере вырастающей атаки
Анализ поведения	Клик-боты, фрод	Долго, дорого, неэффективно	Поможет в аналитике проверить, какие боты остались
История	Широкая, шажок к антифроду	Плохо применим к новым клиентам или устройствам	Стабильность, увеличение стоимости атаки



Методы блокировок
и способы их обхода



Ограничение доступа по IP

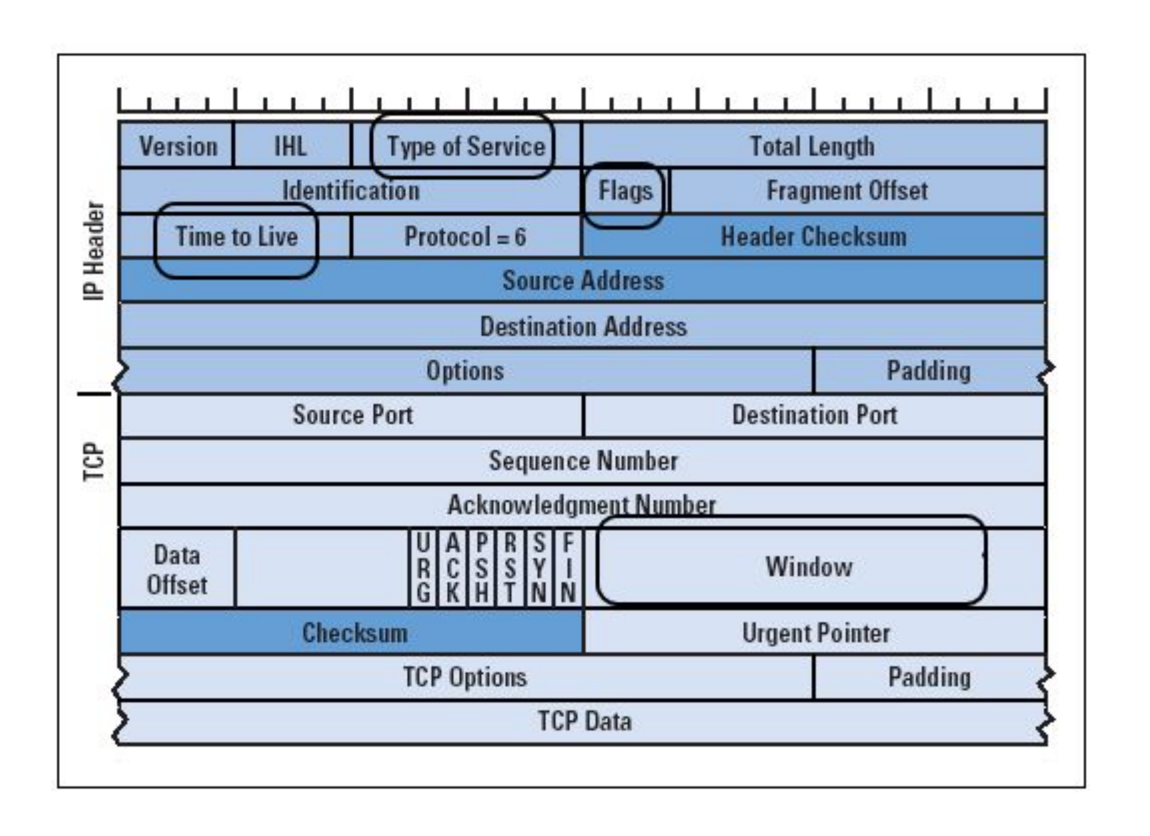
В том числе используя обмен данными (например, с threat Intelligence)

Не панацея, потому что:

- Стоимость proxy очень мала (особенно, если ipv6)
- Подключают операторские proxy
- Используют легитимные IP (ботнеты из роутеров)



По фингерпринтам — SYN



TCP-пакеты, в свою очередь, различаются в зависимости от операционной системы/устройства. Ловят через аналоги p0f

Обходят через OSfooler-ng



По фингерпринтам — TLS

```
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 520
    ▼ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 516
        Version: TLS 1.2 (0x0303)
      ▶ Random: c6812222d3d8b07ca68264c1074cfbc9c9ca097ceae784bc…
        Session ID Length: 32
        Session ID: f0e8fb5ea20a045be755526978180525dba037f725d27c79…
        Cipher Suites Length: 34
      ▶ Cipher Suites (17 suites)
        Compression Methods Length: 1
      ▶ Compression Methods (1 method)
        Extensions Length: 409
      ▶ Extension: Reserved (GREASE) (len=0)
      ▶ Extension: server_name (len=25)
      ▶ Extension: extended_master_secret (len=0)
      ▶ Extension: renegotiation_info (len=1)
      ▶ Extension: supported_groups (len=10)
      ▶ Extension: ec_point_formats (len=2)
      ▶ Extension: session_ticket (len=208)
      ▶ Extension: application_layer_protocol_negotiation (len=14)
      ▶ Extension: status_request (len=5)
      ▶ Extension: signature_algorithms (len=20)
      ▶ Extension: signed_certificate_timestamp (len=0)
      ▶ Extension: key_share (len=43)
      ▶ Extension: psk_key_exchange_modes (len=2)
      ▶ Extension: supported_versions (len=11)
```

Фингерпринт SSL/TLS-клиентов.

Разные библиотеки поддерживают разные шифры и расширения, из них можно слепить уникальный фингерпринт (как ja3)

TLS-фингерпринты - обходятся через такие инструменты как CycleTLS



Аномалии в HTTP



- Назвался груздем — умей в поддержку HTTP 2/QUIC.
- Поддерживай security-фичи (SOP, HSTS, CSP)
- Умей в brotli
- Правильно сортируй заголовки и т.д.

Для обхода — воспроизводят запросы браузера. Но легче использовать сам браузер.



По фингерпринтам — окружение браузеров

Platform

Screen Resolution

Installed fonts

Time zone

Plugins

Color Depth

Is Adblock set or not

CPU class

Pixel ratio

Поддерживаемые API, информацию из браузера, все до чего можно дотянуться — тысячи их. Собирают легитимное окружение чем-то типа fingerprintjs.

Переопределяют в phantomjs/chrome headless.



Что по итогу

Все методы одинаково хороши, но есть нюансы.

В связке работают лучше, чем раздельно.

Необходимо вести скоринговую модель принятия решений.

Нельзя использовать логику на клиентской стороне.

Напрашивается ведение базы хороший/плохой бот.



Всякие умные надписи



Трудно найти, легко потерять, невозможно забыть

Нужно понимать, сколько вы теряете, а может в вашем случае большую часть выручки делают боты?



Защищать дешевле, чем атаковать

Вы занимаетесь бизнесом. Но создатели ботов тоже зарабатывают — это их бизнес, только другой. Просто иногда для этого они используют ваш сервис.



Защита — это увеличение стоимости атаки

Взломать или обойти можно всё, как правило, это вопрос ресурсов. Поэтому атаковать будут всегда, но защищенную систему атаковать менее рентабельно.



Security through obscurity*

Блокировка - не лучший вариант. Давая обратную связь, злоумышленник использует другие методики.

Лучше не допускать гонку вооружений.



Принципы защиты

- Нужны правильно приготовленные рейт-лимиты
- Дешевые метрики — тоже работают (TLS, версии HTTP)
- Внедрять защиту по мере присутствия проблем
- Затрудняем нападение, не давая обратную связь

  (в идеале, чтобы злоумышленник не знал, что он вообще заблокирован)





Вопрос залу

При A/B-тестировании дизайна старый вариант всегда лучше, чем новые тестируемые.

Как на это могут влиять боты и почему?



Про будущее — WebAuthn, Apple Passkey

Safari File Edit View History Bookmarks Window Help

Mon Jun 6 9:41 AM

porcunia.com

Sign In Cancel

Do you want to save a passkey for "chella_boehm@icloud.com"? Passkeys are saved in your iCloud Keychain and are available for sign in on all your devices.

Continue with Touch ID

Other Options



Обратная связь
и комментарии по
докладу по ссылке

Умеешь в
архитектуру сложных
вещей?
hr@antibot.ru





t.me/webpwn